THE EC 'SAFEC' PROJECT: ATEX MEETS IEC 61508

Jill Wilday*, Tony Wray** and Simon Brown***
*Health and Safety Laboratory, Harpur Hill, Buxton, UK
**Health and Safety Laboratory, Broad Lane, Sheffield, UK
***Health and Safety Executive, Stanley Precinct, Bootle, UK

Some types of electrical equipment intended for use in potentially explosive atmospheres rely on so-called 'safety devices' to reduce the likelihood of the equipment presenting a source of ignition which could cause an explosion. Examples of safety devices are motor protection circuits (to limit temperature rise during stall conditions) and pressurisation systems (to prevent ingress of an explosive atmosphere into an electrical equipment enclosure). The EC SAFEC project had the objective of producing a methodology for deciding how to determine the requirements for safety devices to achieve compliance with the ATEX Directive (94/9/EC). Candidate control system standards for categorising the safety devices were EN 954 and IEC 61508 (now EN 61508).

For simple safety devices, EN 954 is sufficient. However, more complex safety devices, particularly if programmable, are better thought of as safety-related systems, and IEC 61508 is appropriate. This requires that the safety device is specified in terms of a safety integrity level (SIL). Three approaches were used to calibrate the SIL required in the different ATEX equipment categories: use of individual risk criteria; use of accident statistics; and estimation of the SIL for a generic design of pressurisation equipment. Further case studies tested the proposed methodology for determining the SIL for a diode safety barrier, a level detection device and both pressure and temperature safety devices. The SAFEC project and its results are described, particularly in terms of how to determine the SIL required in a particular application.

KEYWORDS: IEC 61508; ATEX; Safety integrity; Risk assessment

INTRODUCTION

Some types of electrical equipment intended for use in potentially explosive atmospheres rely on so-called 'safety devices' to reduce the likelihood of the equipment presenting a source of ignition which could cause an explosion. Examples of safety devices are motor protection circuits (to limit temperature rise during stall conditions) and pressurisation systems (to prevent ingress of an explosive atmosphere into an electrical equipment enclosure). The approval and certification of electrical apparatus for potentially explosive atmospheres requires that, where such safety devices are used to reduce the risk of explosion, an assessment be made of their suitability for the intended purpose from a functional safety viewpoint. This needs to be expressed in terms of some measure of confidence that the devices will be able to maintain a required level of safety in accordance with the requirements of the EC ATEX Directive[1], CENELEC standards for electrical apparatus for use in potentially explosive atmospheres[2–9] and relevant standards for safety-related electrical control systems.

CENELEC identified the need for research to determine whether existing and proposed standards in the field of safety-related control systems are suitable for this purpose, and to develop a methodology which will provide the required support for the approval and certification process. Research proposals on this topic were invited under the Standardisation, Measurement and Testing (SMT) Programme and the SAFEC project (contract SMT4-CT98-2255) was selected for funding. It ran from January 1999 to May 2000.

The partners in the SAFEC project were the Health and Safety Laboratory of the Health and Safety Executive (HSL) in the UK (the project coordinator), the Deutsche Montan Technologie (DMT) in Germany, the National Institute for Industrial Environment and Risks (INERIS) in France and the Laboratorio Oficial J.M. Madariaga (LOM) in Spain. The SAFEC partners worked cooperatively with the members of CENELEC Technical Committee 31, Working Group 09 (WG09), which is drafting a standard on "Reliability of safety-related devices" with the intention that the SAFEC results be utilised by WG09 in this standard. Several joint meetings were held.

The SAFEC project comprised six tasks:

1. Derivation of target failure measures (all/HSL).
2. Assessment of current control system standards with reference to the target failure measures from Task 1 (HSL).
3. Identification of safety devices currently used with reference to CENELEC standards (LOM).
4. Study of a selection of safety devices identified in Task 3 (INERIS).
5. Determination of a methodology for testing, validation and certification (DMT).
6. Production of a final report[10] (all/HSL).

This paper concentrates on the choice of control system standards and the calibration of target failure measures for safety devices according to those standards. This work was particularly carried out during tasks 2, 4 and 6.

REQUIREMENTS OF ATEX DIRECTIVE

The ATEX product Directive[1] defines two Groups of application of electrical equipment, each of which has Categories of electrical equipment according to the level of protection required:

- Group I comprises mining applications where the flammable material is methane (firedamp) or flammable dust:
    - Category M1 means that the equipment is required to remain functional in an explosive atmosphere.
    - Category M2 equipment is intended to be de-energised in the event of an explosive atmosphere.

- Group II comprises other applications where equipment is to be used in a potentially explosive atmosphere:
    - Category 1 equipment is intended for use where explosive atmospheres are present continuously, for long periods of time or frequently (referred to elsewhere as Zone 0 and/or 20).
    - Category 2 equipment is intended for use where explosive atmospheres are likely to occur (referred to elsewhere as Zone 1 and/or 21).
    - Category 3 equipment is intended for use where explosive atmospheres are less likely to occur, and if they do occur, do so infrequently and for only a short period of time (referred to elsewhere as Zone 2 and/or 22).

The ATEX product Directive fault tolerance requirements can be summarised as follows:

- A fault tolerance of at least 2 is required for the means of protection of Category 1 equipment.
- A fault tolerance of at least 1 is required for the means of protection of Category 2 equipment.
- No fault tolerance is required for the means of protection of Category 3 equipment.

The SAFEC project regarded a ‘safety device’ as a part of the equipment, which has an autonomous safety function with respect to the risk of explosion.

CHOICE OF CONTROL SYSTEM STANDARDS

Task 2 of the SAFEC project, carried out by HSL, included a review of existing control system standards, with reference to the requirements of the ATEX product Directive[1]. Since safety devices are defined as having an autonomous safety function (or controlling function), it was expected that control system standards might be useful in defining the requirements for safety devices. There are two standards which provide guidance on the design of control systems for use in safety-related applications: EN 954-1[11]; and IEC 61508[12] (now also published as EN 61508).

A discussion of the relative merits of the two standards for this purpose has been published previously[13]. EN 954 can be used for simple safety devices, e.g. non-programmable electrical interlocks, especially where the appropriate CENELEC standard refers to EN 954. However, it was recognised that some existing CENELEC standards make reference to EN 954 in cases where nowadays it would be more appropriate to refer to IEC 61508, particularly for complex or programmable electronic safety devices (such as a pressurisation control system using a programmable logic controller). Therefore, it was proposed[10] that any industry-specific standard for complex and programmable safety devices should be based on IEC 61508 but have an additional requirement, based on fault tolerance, which will ensure that the fault tolerance requirements of the ATEX Directive are met. However, it was also recognised that some safety devices may already be fully specified within relevant CENELEC standards, e.g. references 2–9. In these cases, it may not be necessary to further specify the safety device in terms of IEC 61508 or EN 954.

In considering the requirements for safety devices according to these two standards, it is useful to define the equipment under control (EUC), according to IEC 61508, as that part of the equipment (as defined by the ATEX Directive) which is not the safety device. See Figure 1.

CALIBRATION OF REQUIRED IEC 61508 SAFETY INTEGRITY LEVELS

INTRODUCTION

IEC 61508 defines safety integrity levels (SIL) for safety functions by taking into account:

- quantified reliability of the safety function (see Table 1). The quantified analysis of a system deals with the random hardware failure rate;
- qualitative reliability. The techniques used to design, maintain, etc. the system throughout its lifecycle must be sufficient to ensure that the rate of systematic failures is less than the random hardware failure rate; and
- architectural constraints, based on fault tolerance and fail-to-safety characteristics. These put a ceiling on the safety integrity level (SIL) that can be claimed for any particular system in order to ensure that uncertain reliability calculations, e.g., where reliability data are sparse, do not lead to an inflated SIL (see Table 2).

Table 1. Quantitative reliability requirements of IEC 61508

SIL	Probability of failure on demand (for low demand rate operation)	Frequency of failure (per hour) for continuous operation
4	10^{-5}–10^{-4}	10^{-9} –10^{-8}
3	10^{-4}–10^{-3}	10^{-8}–10^{-7}
2	10^{-3}–10^{-2}	10^{-7}–10^{-6}
1	10^{-2}–10^{-1}	10^{-6}–10^{-5}

Table 2. Architectural constraints of IEC 61508

Safe failure fraction	Hardware fault tolerance		
	0	1	2
For type A safety-related subsystems			
<60%	SIL1	SIL2	SIL3
60%–<90%	SIL2	SIL3	SIL4
90%–<99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4
For type B safety-related subsystems			
<60%	not allowed	SIL1	SIL2
60%–<90%	SIL1	SIL2	SIL3
90%–<99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

The early stages in the IEC 61508 lifecycle involve carrying out hazard and risk assessment and allocating safety requirements to relevant safety functions. It was necessary within SAFEC to define or calibrate the SIL required for each ATEX equipment category. A target SIL requirement applies to a particular safety function, not to a safety device. The safety function may be implemented by a range of technologies and each may achieve a part of the required risk reduction. This is illustrated in Figures A.1 and A.2 of Part 3, Annex A of IEC 61508[12], on which Figure 2 is based.

In calibrating the required SIL, a useful hypothetical concept was a safety function protecting against a case in which there is a source of ignition in normal operation. However, this would not, of course, be a practical design for equipment intended for use in potentially explosive atmospheres.

Three approaches were used to calibrate the SILs required:

- Use of individual risk criteria to determine the necessary risk reduction;
- Use of accident statistics to attempt to determine the SIL for existing equipment;
- Estimation of SILs of safety devices within existing equipment.

These are discussed in more detail in the following sections.

INDIVIDUAL RISK

A convenient quantitative definition of hazardous zones, in terms of the time that flammable gas would be expected to be present, is given by Table 3[14]. In all cases, the probability of occurrence of a flammable atmosphere corresponds to the worst-case probability for the particular zone. It should be noted that these values have not been well accepted in all industrial sectors so, although they have been considered by CENELEC working groups, they have not been incorporated in standards.

Calculations of required risk reduction and hence SIL are shown in Table 4 for a range of risk criteria. The criteria range from intolerable (10^{-3} per year) to broadly acceptable (10^{-6} per year)[15]. A criterion of 10^{-5} per year has been used in previous work by the Institute of Petroleum[16].

Table 3. Probability of an explosive atmosphere being present

Zone	Quantitative assumption (hrs/yr)	Probability of occurrence (%)
0	> 1000	100
1	< 1000 and > 100	10
2	< 10	0.1

Table 4. Coarse estimate of integrity requirement based on risk tolerability criteria

					Unit
Criterion for probability of death	10^{-3}	10^{-4}	10^{-5}	10^{-6}	per year
Number of workers/members of the public present[a]	0.2	0.2	0.2	0.2	
Required risk reduction:					
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 0	0.57	0.057	0.006	0.0006	per 10^6 hrs
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 1	5.7	0.57	0.06	0.006	per 10^6 hrs
Maximum possible failure frequency, assuming a continuous source of ignition, Zone 2	570	57	5.7	0.57	per 10^6 hrs
Equivalent safety integrity requirement:					
SIL required to achieve target[b], Zone 0	SIL2	SIL3	SIL4	SIL5[c]	
SIL required to achieve target, Zone 1	SIL1	SIL2	SIL3	SIL4	
SIL required to achieve target, Zone 2	SIL1[d]	SIL1[e]	SIL1	SIL2	

Notes to Table 4:
[a]This assumes 20 deaths per 100 explosions involving pressurisation systems[16, 17]
[b]This is the SIL of the overall safety function and includes all protection measures/devices. It is based directly on the maximum allowable failure frequency of the safety function, from the rows above, and assumes continuous operation of the safety function with the SIL taken from Table 1.
[c]SIL5 is outside the range of achievable SILs considered by IEC 61508; however, SIL 5 has been used here in order to make the table more meaningful.
[d and e]SIL1 represents the minimum integrity requirement of IEC 61508 for a system defined as being safety-related; therefore, SIL1 must apply to these positions.

ACCIDENT STATISTICS

Discussion with a UK manufacturer of pressurization systems has indicated that about 18,000 such systems have been put into service in the UK over the past 20 years. Assuming a life expectancy in the region of 8 years, this suggests an average of about 6,000 systems have been in use over this time. The partners were not aware of any explosions resulting from the failure of a pressurization system. Therefore, this sets a lower limit on the integrity of pressurization systems over the past 20 years, as shown in Table 5, below. The values in Table 5 were calculated on the assumption that, if no explosions occur over N operating hours, then a reasonable assumption is that the probability of an explosion occurring in the next N operating hours is 0.5.

Table 5 suggests that the integrity of existing pressurization systems is:

Table 5. SIL indications from accident records

	Assumed zone of operation[a]			
	Zone 1H[b]	Zone 1L[b]	Zone 2	Units
Period of study	20	20	20	years
Number of systems in use in the UK over this period	6,000	6,000	6,000	
Total operating period	1,051,920,000	1,051,920,000	1,051,920,000	system-hours
Probability of gas presence[c]	0.032	0.0032	0.00032	
Operating period with gas present	33,661,440	3,366,144	336,614	"gas" hours
Number of known explosions	0	0	0	
Indicated dangerous failure rate for each system	0.015	0.15	1.5	per 10^6 hrs
Indicated SIL for the overall safety system[d]	SIL3	SIL2	SIL1	

Notes to Table 5:

[a] The data in each of the columns have been calculated on the basis that all systems were used in the single specified zone.

[b] For the purpose of these calculations, Zone 1 has been split into two regions.

[c] It would be inappropriate to use the worst-case probabilities for the presence of flammable gas in the calculations in this particular table, as we must use an estimate of the actual probability. Without any prior knowledge of the distribution of this probability, the logarithmic mean of the range of probabilities covered by each (sub) zone has been used. This is: Zone 1H - 3.2%; Zone 1L - 0.32% and Zone 2 - 0.032%.

[d] This is the average SIL of the total configuration of safety-related systems. The pressurization control system (e.g., purge and shutdown systems) will contribute to this SIL together with other systems, e.g., the air supply.

SIL1, if they have been mainly used in Zone 2;

SIL2, if they have been mainly used at the lower end of Zone 1, or

SIL3, if they have been mainly used at the upper end of Zone 1.

However, as the probability of gas in the majority of Zone 1 environments will probably lie near the lower end of the zone (i.e., Zone 1L as shown in Table 5) with few at the upper end (shown as Zone 1H), Table 5 should not be considered to indicate that existing pressurization systems are able to achieve SIL3.

ESTIMATION OF SIL FOR SAFETY DEVICES ON EXISTING EQUIPMENT

Again, it can be assumed that existing certified electrical equipment is of adequate integrity, given that there is no history of explosions which have been initiated by certified electrical equipment. Therefore the SILs of existing safety devices can be assumed adequate. SILs for the following safety devices have been estimated (on the basis of random hardware failures only) during the SAFEC project[10] and results are given in Table 6 below.

- Two safety functions within a pressurisation system.
- Diode safety barrier.
- Level detection safety device.
- Pressure and temperature safety devices.

An example is provided by one of the safety functions for the pressurisation system. A generic design of pressurisation equipment was provided by a manufacturer (see Figures 3 and 4). One of the safety functions was to purge the enclosure prior to power being allowed to the equipment within it. The estimation of SIL took account only of the quantitative reliability aspects and the calculation is summarised in Table 6. Reliability data from Smith[18] was used.

Table 6. Determination of failure rate of purging delay function

Component	Failure mode	Failure rate, etc.	Unit	Comments
Contactor K	Energized state. Assumes power circuit correctly fused.	0.400	per 10^6 hrs	Assume 10% failure to open
RY2	Energized state	0.030	per 10^6 hrs	Armature. 10% failure to open.
Discriminator A	Output high	0.120	per 10^6 hrs	Bipolar linear
Capacitor C	Reduced capacitance	0.300	per 10^6 hrs	Assume aluminium electrolytic.
Circuit board	Ignored as de-energized = safe state	0.000	per 10^6 hrs	

Diode D	Short circuit	0.006	per 10^6 hrs	Assume 15% to short-circuit
Resistor Rb	Short circuit/ reduced resistance	0.000	per 10^6 hrs	Not credible
Resistor Ra	Open circuit/ increased resistance	0.002	per 10^6 hrs	Assume 50% to drift
Flow sensor AND Pressure sensor	Contacts-closed-β-factor of 0.05 assumed	0.050	per 10^6 hrs	
Overall failure rate: Function 2 (λ)		0.908	per 10^6hrs	
Proof test interval, T (six months)		4,383	hours	
Probability of failure on demand (λT/2)		1.99	$*10^{-3}$	
Safety integrity level of Function 2		SIL2		

Because the frequency of access to the pressurized cabinet is likely to be significantly less than the proof test interval, at first sight it may be assumed that failures of the purging function are unlikely to be revealed by the proof tests. However, this does not take into account that there may be no gas present when the pressurized cabinet is opened, and that the person opening the pressurized cabinet will be able to smell the flammable gas (unless this is, for example, hydrogen) at a level well below the lower explosive limit. If these are taken into account, a demand on the purging function (i.e., when the cabinet has been opened in the presence of flammable gas) occurs less often than the proof tests as is shown in Table 6, which determines the explosion rate from the failure rate of the purging function.

SUMMARY OF ESTIMATIONS OF SIL

A summary of the results of the above calculations for the purpose of calibrating the target risk reduction (SIL) requirement are given in Table 7. It can be that there is a good degree of convergence between the different methods of calibrating the target risk reduction requirements for the different hazardous zones. The approach of the SAFEC project has been to find targets which are in line with published risk tolerability criteria and are also achievable by existing safety devices. The lack of any history of explosions ignited by certified electrical equipment strongly suggests that current designs of safety devices are adequate.

It is proposed that the target risk reduction requirements, for the safety function of protecting against a hypothetical case in which there is a source of ignition in normal operation, be defined according to Table 8.

It is very important to note that these target risk reduction requirements refer to the safety function and not to the safety device. The safety function may be partly achieved by design features of the certified electrical equipment other than the safety device. Indeed, for certified electrical equipment, such design features will usually be present to prevent there being a source of ignition during normal operation. The necessary risk reduction can be allocated between available safety systems, including the safety device (see Figure 2).

Table 7. Summary of calculations for calibrating target risk reduction requirement

	Target risk reduction requirement		
Description of method	Zone 0	Zone 1	Zone 2
Use of individual risk criteria	SIL 3	SIL 2	SIL 1
Use of accident statistics applied to pressurised systems		SIL 2 or SIL 3	SIL 1
Estimated SIL for pressurisation system. Turn off equipment if pressurisation fails.		SIL 2 or SIL 3 (Note a)	
Estimated SIL for pressurisation system. Purge before allowing power onto equipment		SIL 2 (Note b)	
Estimated SIL for diode safety barrier	SIL 4		
Estimated SIL for low level detection system			SIL 1 (Note c)
Estimated SIL for pressure safety device		SIL 2 (note d)	
Estimated SIL for temperature safety device		SIL 2 (note e)	SIL 2 (Note e)

Notes for Table 7

(a) SIL 3 is possible given a suitably reliable air supply.

(b) The overall integrity could be increased by suitable operating procedures, such that SIL 3 may also be possible.

(c) The assumed application was within an LPG tank. This will usually be non-flammable (above UFL) and will therefore correspond to Zone 2.

(d) This could be increased given a suitably reliable air supply (see 5.4.1)

(e) The temperature safety device is assumed to be on a motor intended for use in either Zone 1 or Zone 2.

Table 8. Proposed target risk reduction requirements for the hypothetical case of protecting against an ignition source during normal operation

Hazardous zone	ATEX equipment categories	Target SIL requirement
0 or 20	1	SIL 3
1 or 21	2	SIL 2
2 or 22	3	SIL 1

Table 9 gives the proposed SIL requirements for safety devices as a function of the hazardous zone and the fault tolerance of the equipment under control.

Table 9. Proposed IEC 61508 safety requirements for safety functions

Hazardous area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Fault tolerance requirement of ATEX Directive	2			1			0	
Equipment (EUC) fault tolerance	2	1	0	1	0	–1	0	–1
SIL of the safety function that the monitoring or control unit is providing	-	SIL 2	SIL 3	-	SIL 1	SIL 2	-	SIL 1
Resulting equipment category (under ATEX) of the combination	category 1			category 2			category 3	

CALIBRATION OF REQUIRED EN 954 CATEGORIES

It was concluded above that simple safety devices should meet the EN 954 category, which achieves the relevant ATEX fault tolerance requirement. A suggested definition of “simple safety device” is one which is simple enough that all the failure modes can be identified.

EN 954 has 5 categories for describing control systems:

- Category B has a fault tolerance of 0;
- Category 1 has a fault tolerance of 0;
- Category 2 has a fault tolerance of 0 but has automatic monitoring;
- Category 3 has a fault tolerance of 1, and
- Category 4 has:
    - a fault tolerance of 1 with automatic monitoring, **or**
    - a fault tolerance of 2 or more.

It therefore follows that the mapping between ATEX equipment categories and EN 954 categories for the safety devices is as given in Table 10. (Note that the addition of a safety device with a fault tolerance of zero to equipment with a fault tolerance of zero gives an overall fault tolerance of one.) In Table 10, the category of the safety device depends on the fault tolerance of the EUC.

Table 10. Proposed EN 954 requirements for simple safety devices

Hazardous area	Zone 0 Zone 20			Zone 1 Zone 21			Zone 2 Zone 22	
Fault tolerance requirement of ATEX Directive	2			1			0	
Equipment (EUC) fault tolerance	2	1	0	1	0	–1	0	–1
EN 954 category of the safety device	-	B, 1, 2, 3 or 4	3 or 4	-	B, 1, 2, 3 or 4	3 or 4	-	B, 1, 2, 3 or 4
Resulting equipment category (under ATEX) of the combination	ATEX category 1			ATEX category 2			ATEX category 3	

Note that a fault tolerance of "–1" implies that the equipment would be incendive in normal operation, without the intervention of the safety device

CONCLUSIONS

1. Safety devices, as defined under the ATEX Directive[1] have an autonomous safety function. They include implementation in a number of technologies and can be specified in a number of ways:
    - Devices which are already fully defined in CENELEC standards, e.g. references 2–9.
    - Simple safety devices, which can be defined according to EN 954[11].
    - More complex devices, which are generally electric/electronic/electronic programmable in nature and can be defined according to IEC 61508[12].
2. Proposed requirements for safety devices specified under IEC 61508 or EN 954 have been derived and are given in Tables 9 and 10, respectively.

REFERENCES

1. Directive 94/9/EC of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres, Official Journal of the European Communities, 19/4/94
2. EN 50014 Electrical apparatus for potentially explosive atmospheres. General requirements.
3. EN 50015 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode "o" oil immersion.
4. EN 50016 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : pressurised apparatus "p".

5. EN 50017 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : powder filling “q”.
6. EN 50018 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : flameproof enclosure “d”.
7. EN 50019 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : increased safety “e”.
8. EN 50020 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : intrinsic safety “i”.
9. EN 50028 Electrical apparatus for potentially explosive atmospheres. Specific requirements for the protective mode : encapsulation “m”.
10. Wilday, A J et al., (2000), “Determination of safety categories of electrical devices used in potentially explosive atmospheres (SAFEC) Final Report”, www.safetynet.de/EC-Projects/40.html.
11. BS EN 954-1: 1997, Safety of machinery - Safety-related parts of control systems - Part 1. General principles for design., BSI Standards, ISBN 0 580 27466 7.
12. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7, 1998 (also published as BS EN 61508).
13. Wilday, A J, and Wray, A M, “Safety categories for safety devices used in electrical equipment for use in potentially explosive atmospheres”, Proceedings of International Conference on Explosion Safety in Hazardous Areas, 11–12 November 1999, Institution of Electrical Engineers, UK
14. Area Classification Code for Petroleum Installations (Part 15 of the Institute of Petroleum Model Code of Safe Practice in the Petroleum Industry), Institute of Petroleum/John Wiley, 1990
15. The tolerability of risk from nuclear power stations, HSE/HMSO, 1992.
16. A. W. Cox, F. P. Lees & M. L. Ang, “Classification of hazardous locations”, Institution of Chemical Engineers, 1990
17. BIA, “Dokumentation Staubexplosionen, Analyse und Einzelfalldarstellung”, Report 11/97, 1997
18. Smith, D J (1993), Reliability, maintainability and risk - Practical methods for engineers, Fourth edition, Butterworth Heinemann, 1993, ISBN 0 7506 0854 4.

ACKNOWLEDGEMENTS

The work described was carried out within the EC SAFEC project (SMT4-CT98-2255) with the support of the European Commission. The input of the other partners and of the members of CENELEC TC 31/WG09 is gratefully acknowledged. Information on pressurised systems was kindly provided by Mr A Owler of “Ex” Certification Outsource Ltd.

DISCLAIMER

The views expressed in this paper are those of the authors alone and are not a statement of HSE or HSL policy.

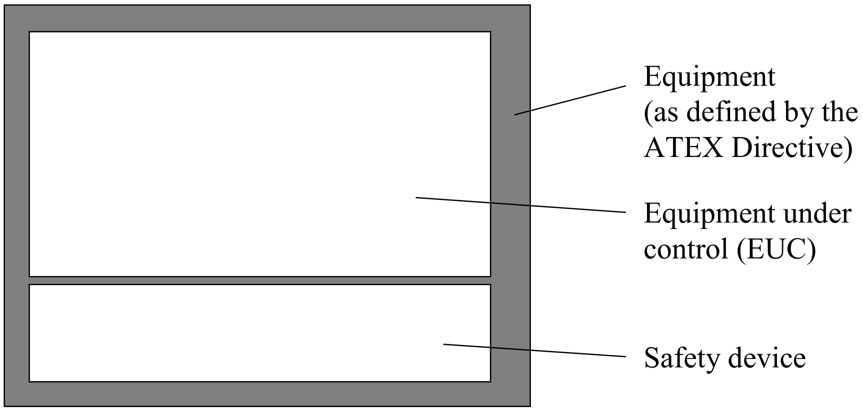
Equipment
(as defined by the ATEX Directive)
Equipment under control (EUC)
Safety device

Figure 1. Definition of terms

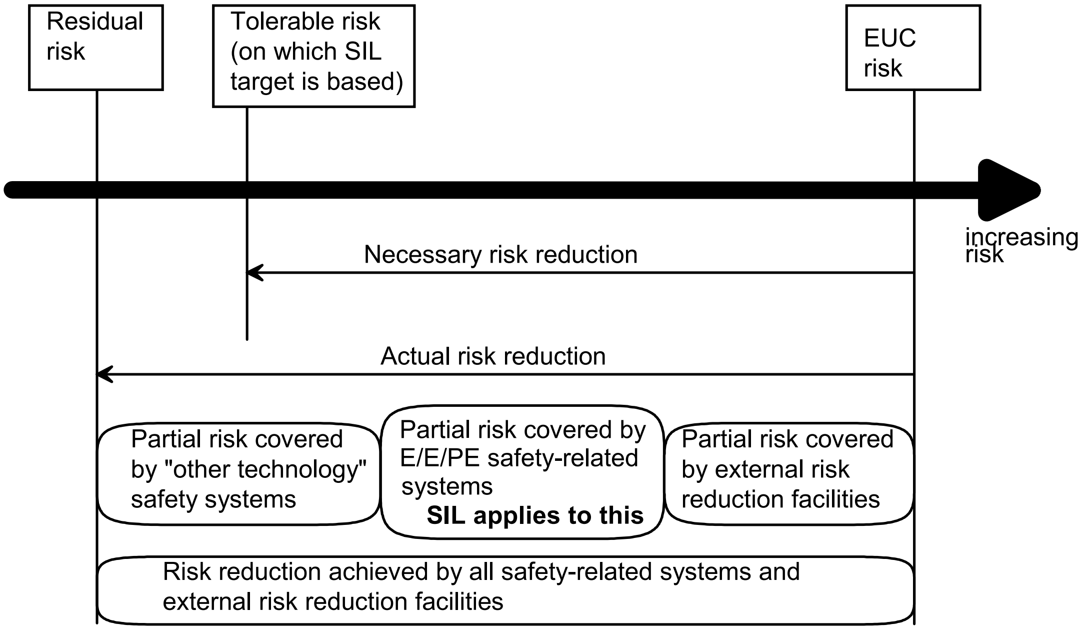
Residual risk
Tolerable risk (on which SIL target is based)
EUC risk
increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk covered by "other technology" safety systems
Partial risk covered by E/E/PE safety-related systems
SIL applies to this
Partial risk covered by external risk reduction facilities
Risk reduction achieved by all safety-related systems and external risk reduction facilities

Figure 2. Risk concepts from IEC 61508

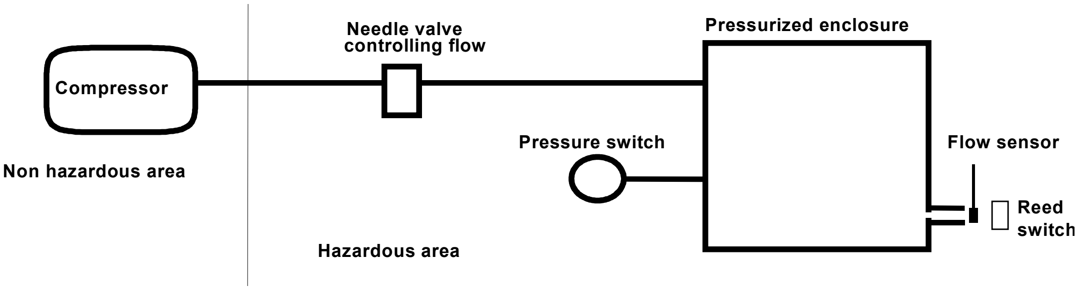

Figure 3. Generic design for a pressurisation system: air-flow diagram

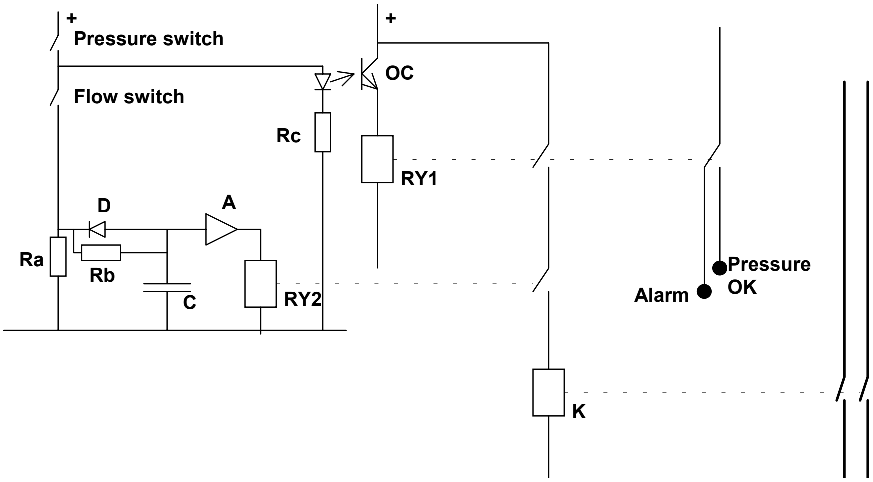

Figure 4. Generic design for a pressurisation system: electrical diagram